



THREATForecast

AND REPORT

The **monthly Spam Soap Threat Forecast & Report** provides IT leaders and messaging security professionals with information on recent and potential email and Web threats. The forecast relies on current and historical data and trends, as well as expert analysis of real time spam and virus events monitored and assessed by the 24x7 Threat Operations Center.

October 2008 Threat Forecast

Spam Levels Hold Steady, Focus Shifts

Overall spam volume is expected to remain steady with spam accounting for approximately 90% of all emailed messages. However, we expect to see a dramatic shift in spam themes away from pharmaceutical spam and luxury items toward themes related to the upcoming Presidential election and the U.S. economy.

Major Economic Spam Attack “Probable”

The recent public and media attention and concern about the economy provides spammers an excellent opportunity to launch a significant and widespread spam attack. We have already observed an increase in malicious messages disguised as Debt-Consolidation and loan offers. These small, isolated spam attacks are often precursors to major outbreaks, as we saw with the recent CNN spam outbreak. Therefore, we anticipate seeing one or several major spam attacks with economic themes in the weeks ahead.

Identity Thief or Identity Protector?

Although we’ve only seen a small number to date, we expect to see an increase in malicious messages claiming to offer identify theft and Internet protection services. This is a relatively new approach, although it’s just another form of social engineering exploiting people’s concerns over the economy and their financial security.

Increased Exploitation of Web 2.0

We anticipate seeing an increased amount of spam attacks aimed at user-driven content models, similar to the abuse seen on the AARP site that Spam Soap reported last month. We also anticipate seeing image hosting services such as Imageshack, Picasa and Flickr being used to host spam content. These image hosting sites make a perfect nesting ground for Image Spam.



September 2008 Threat Report

Following the 15% spike in August, spam levels eased slightly lowering 5% in September. The easing was gradual as we continued to see residual effects from the massive CNN outbreak in early August. Despite the slightly lower volume, spam still accounted for 90.5% of all email messages (91.4% in August).

We've also noticed a disturbing new trend. Since May 2008, we have seen a meteoric rise in the prevalence of email-borne malware, the likes of which have not been seen since the Storm Worm outbreak in 2007. In September, more than 1 in 20 emails contained malware which is a rate 7 times higher than the average between October 2007 and May 2008. Stay tune for more information on this front.

Total Spam Level



90.5%

Down from 91.4% in August

Top 5 Categories of Spam

1. Health
2. Offers
3. Phishing
4. Foreign Language
5. Gambling

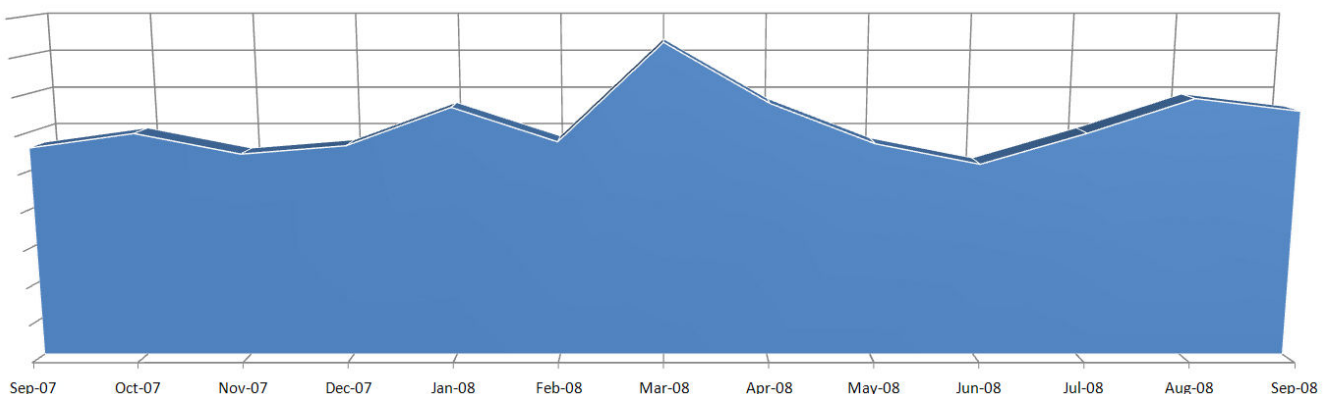
Top 5 Worms/Viruses

1. Troj/Agent-HNY
2. Troj/Invo-Zip
3. Mal/EncPk-ES
4. Troj/Mdrop-BUR
5. Troj/Agent-HLV

Top 5 Spam Countries

1. United States
2. Brazil
3. Russian Federation
4. United Kingdom
5. China

Historical Spam Volume



Most Prevalent Types of Spam

During September, pharmaceutical spam continued to be the most prevalent theme, followed by fake luxury items – watches, handbags, pens, etc. One interesting new development was an increase in the volume of Debt-Consolidation and loan offer spam enticements for identity theft and other types of Internet fraud. We believe this was due to Internet criminals attempting to take advantage of the overall downturn in economic conditions and public feelings of financial insecurity.

Phishing in all its familiar forms

Nigerian/419, Bank, Account Update Requests, etc. – remained a prevalent tactic during September. Gambling spam – enticements leading to actual gambling sites – while nothing new in and of itself, did increase in volume and overall prevalence.

Rogue Anti-Virus Deceptions – “Vista / XP Anti-Virus 2008”

This much-publicized tactic attempts to deceive users into thinking that their Anti-Virus software needs to be updated. If the user falls for the scheme, they unwittingly install malware instead of an AV update, which triggers an ever-increasing variety of malicious behaviors such as adding the computer to a botnet, convincing the user to pay money for non-existent AV subscriptions via Internet payment services, neverending pop-up attacks and disabling of the start menu and certain mouse functionality. This tactic’s appearance is constantly updated and improved to increase its probability of success.

This tactic experienced a resurgence of attention in the media, and we did continue to see examples in September. We expect this tactic to continue to evolve and defraud more users going forward despite attempts to increase public awareness.

Malicious Video-link spam

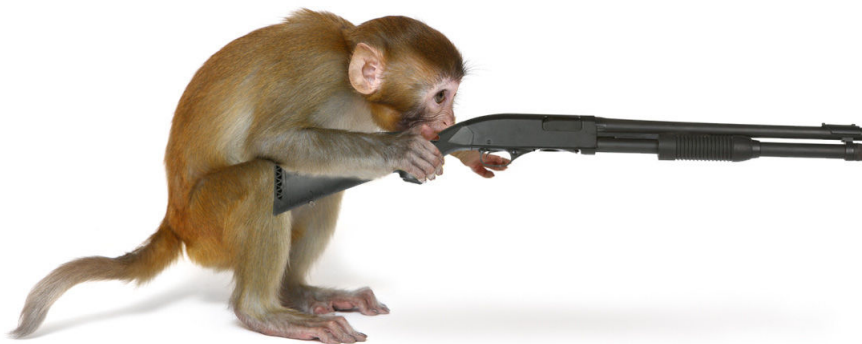
This type of spam continued to be dominated by links pointing to fake video player web sites that mimicked the look and feel of well-known video sites. When the user clicked on the links, they were directed to web sites that would attempt to download various types of malware.



The Best “Worst” Spam of the Month

The single most difficult part of developing the monthly Spam Soap Threat Forecast and Report is choosing a best “worst” spam of the month. There are simply too many to choose from each month. What’s interesting about most of them, is the downright silliness of their headlines. This, of course, raises the question, “Do people actually fall for this stuff?” With that in mind, below is just a short sampling of the more ridiculous spam headlines from the past month.

- Angelina Jolie And Madonna Compete For Adoption Of Jamie Lynn Spears Baby
- Angry man shoots lawnmower
- Both Obama And McCain Claim That They Will Deport Elton John
- Britney Spears And Michael Jackson To Write Parenting Book
- Golden ticket for space trip in chocolate bar
- Young girl throws scorpion at teacher
- GPS-equipped turtle stumbles upon field of marijuana in a D.C. park.
- Grey dogs more likely to kill
- Home Office To Deport Anyone With Iq Below 100
- Michael Jackson is sued by his own dog
- NASA to use Space Shuttles to Kill Birds
- Monkey shoots trainer with tranquilizer



HEADQUARTERS

Spam Soap, Inc.
 3193 Red Hill Avenue
 Costa Mesa, CA 92626
Phone: 866.SPAM.OUT or 866.772.6688
 Outside the US call (001) 714.955.6959
Fax: 949.203.6425
Email: info@spamsoap.com

SALES

sales@spamsoap.com
CHANNEL PROGRAM
channel@spamsoap.com
MARKETING AND REVIEWS
reviews@spamsoap.com